Security Risks Associated with Network Based Physical Security Management Systems

William H. Sawyer, Ph.D.,
Senior Technical Consultant
Radian, Inc.
Alexandria, VA 22303

Introduction

A. The Issue

The evolution of physical security and access control systems has made it possible to integrate them into the corporate network architecture.

Advantages:

- Lower installation and maintenance costs than traditional hardwired systems
- Integrated information between security, HR, and other corporate data
- Ease of use

Disadvantages:

- Security
- Reliability

Introduction

Physical Security System Architectures

Stand alone systems

Hardwired systems with external access through dial-up/dial-back connections

- Expensive to install and maintain
- No unified database with HR and IT
- Very secure system

Introduction

Physical Security System Architecture

Stand alone systems

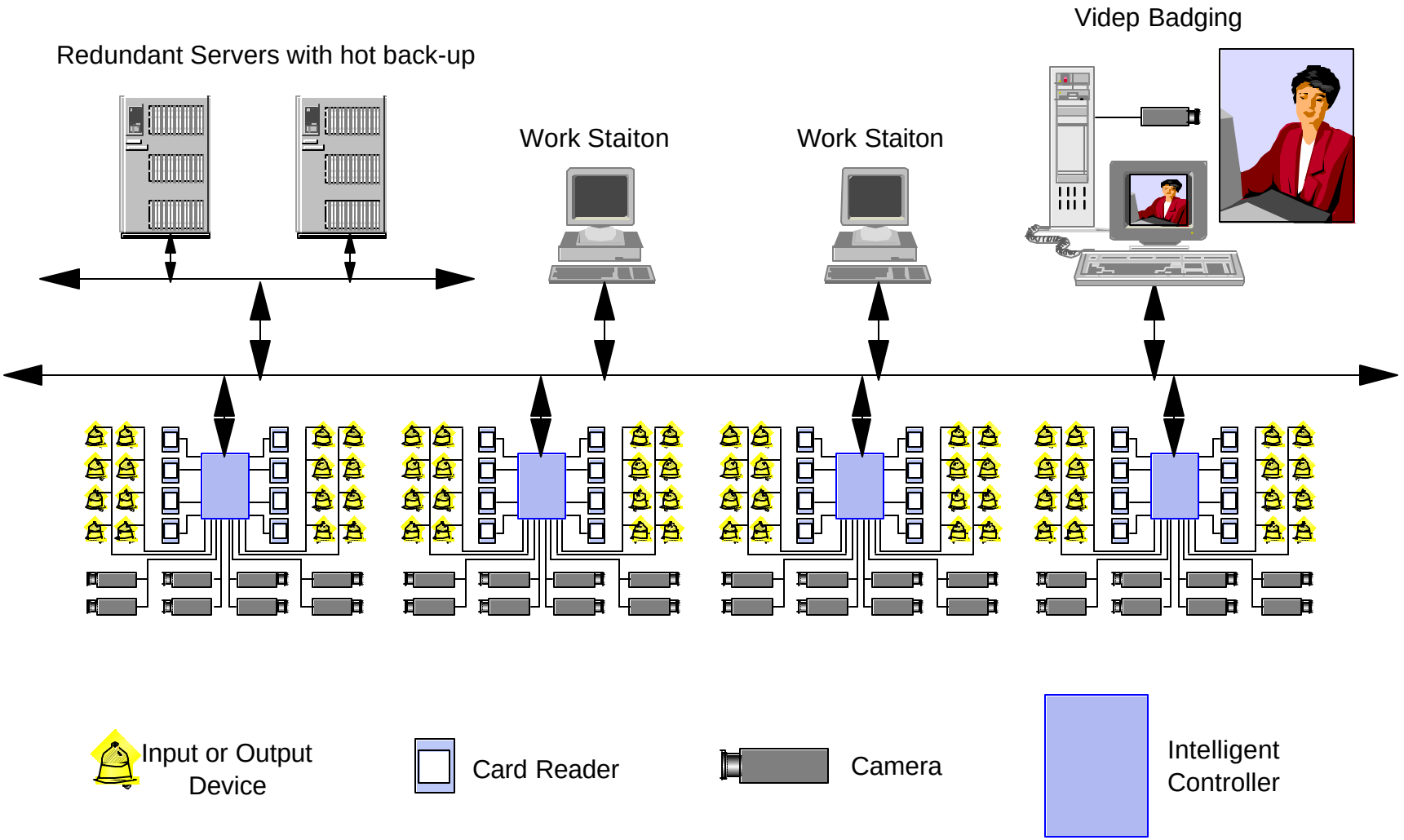
Dedicated LAN

This has most of the `Speed and advantages and disadvantages of a Hardwired system.

» Stability can be a problem depending upon the operating system.

`

Dedicated Security Management System

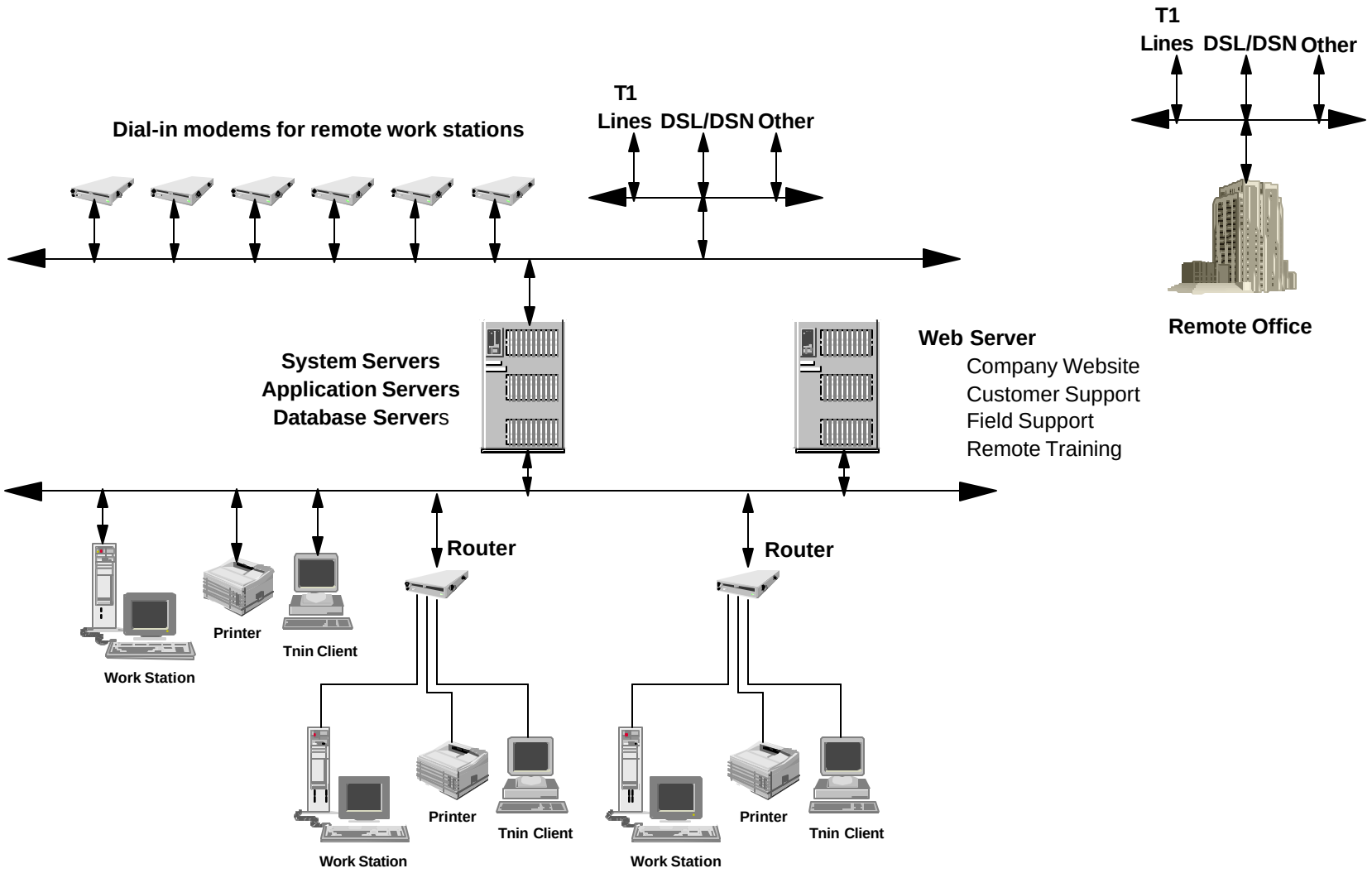


Introduction

A. Standard Network Architecture

2. Connectivity
   a. Hardwired
   b. Dial-in
   c. Web Access
   d. Wireless – 802.11b

Standard Network Architecture



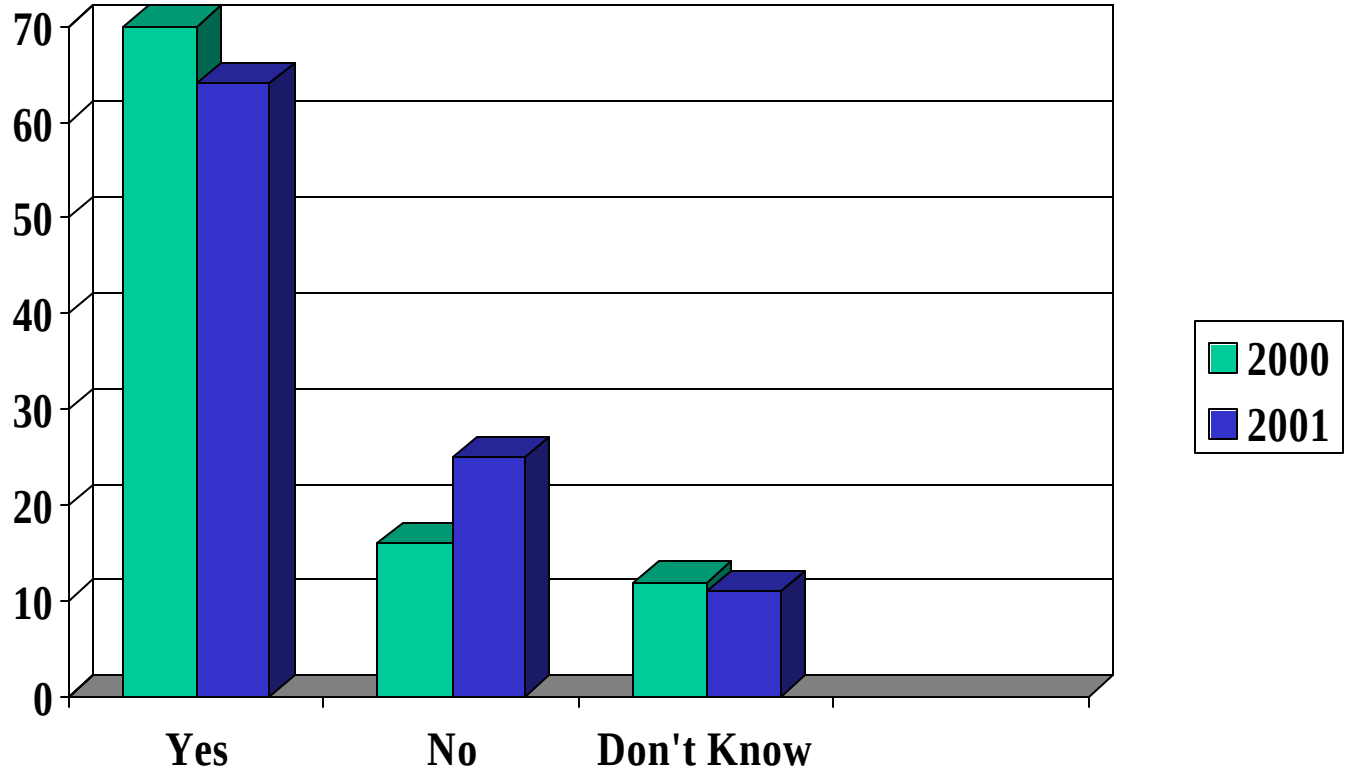
Network Security

Vulnerabilities

- Access to confidential data
- Data modification or destruction
- Denial of service

Network Security

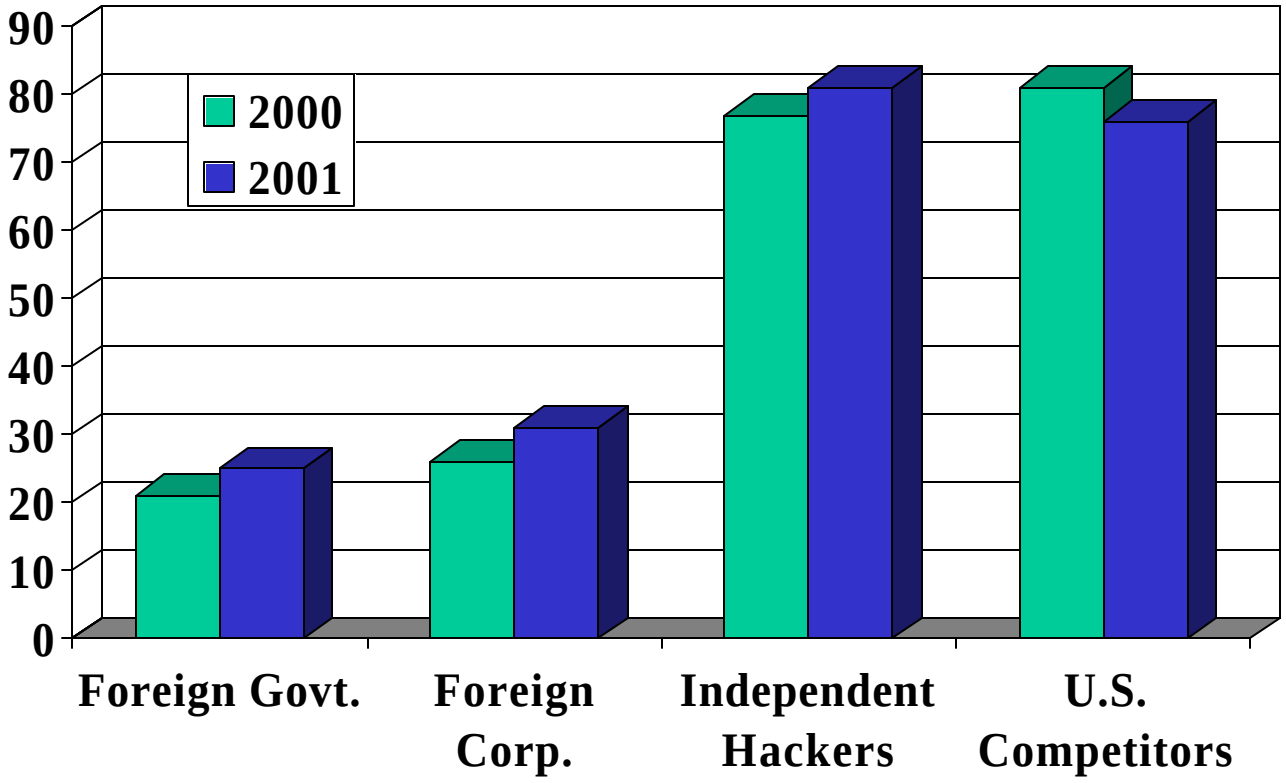
Percentage of 538 computer security practitioners in U.S. Corporations, government agencies, financial institutions, medical institutions, and universities experiencing a network break-in.



6th Annual Computer Crime and Security Survey, Computer Security Institute /FBI Survey

Network Security

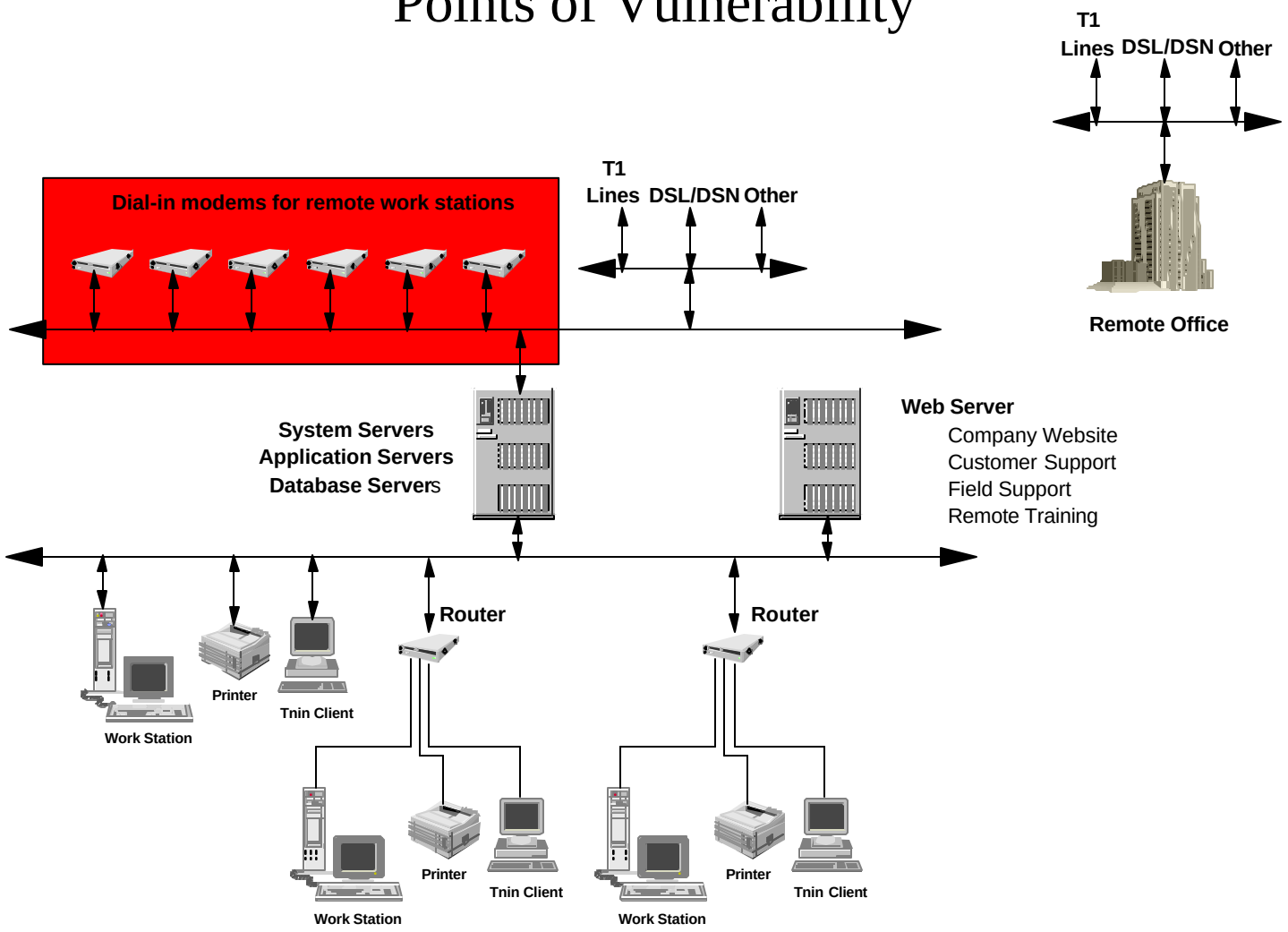
External Threats



6th Annual Computer Crime and Security Survey, Computer Security Institute /FBI Survey

Typical Enterprise LAN/WAN

Points of Vulnerability

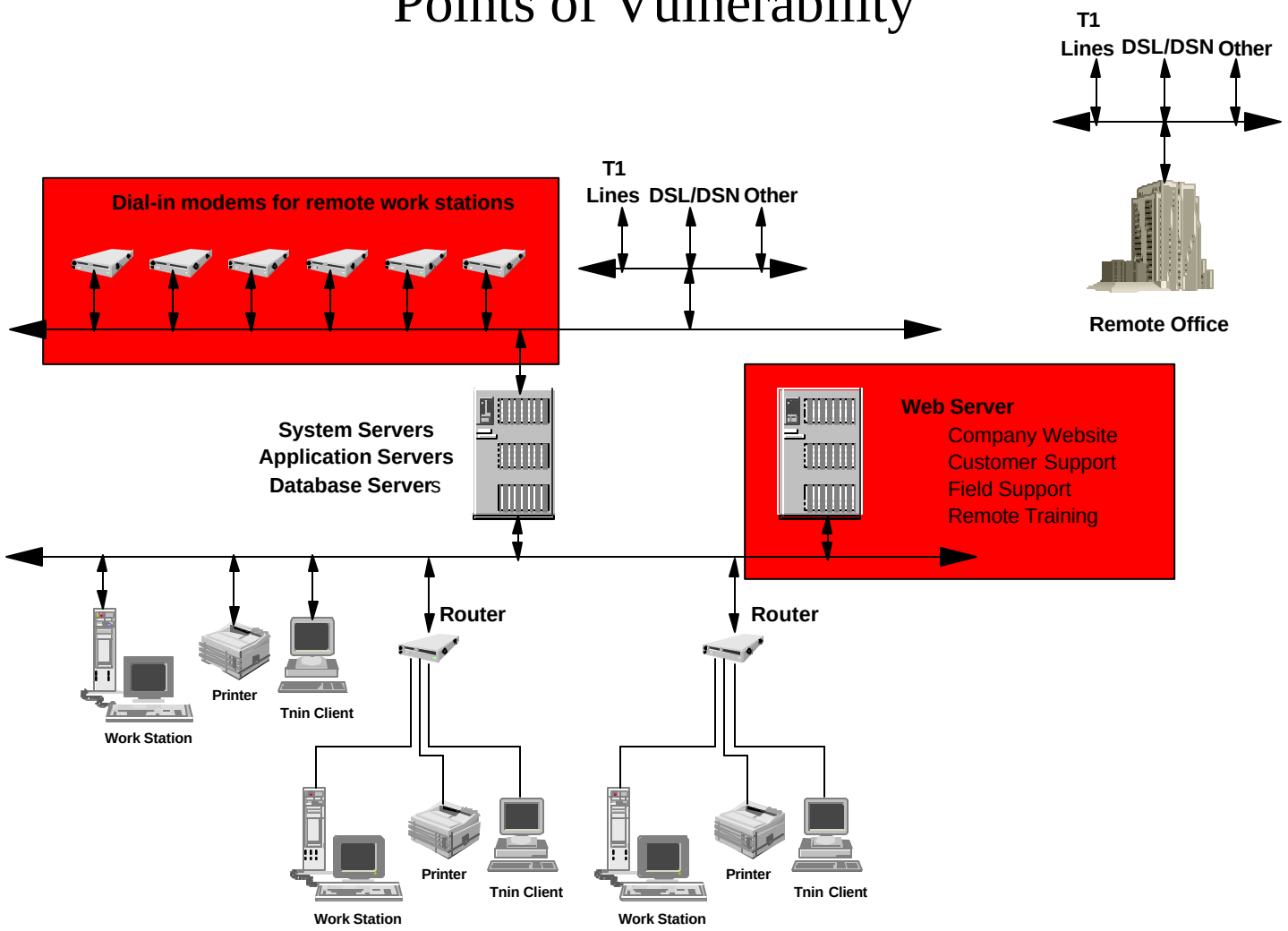


External Vulnerabilities

- Remote Dial-in
  - Simple password protection is not sufficient
    - Encrypted passwords are better
    - Password plus token is good security
      - Card
      - Synchronized counter
      - Biometric device
    - Automatic Dial-back to prearranged number

Typical Enterprise LAN/WAN

Points of Vulnerability



External Vulnerabilities

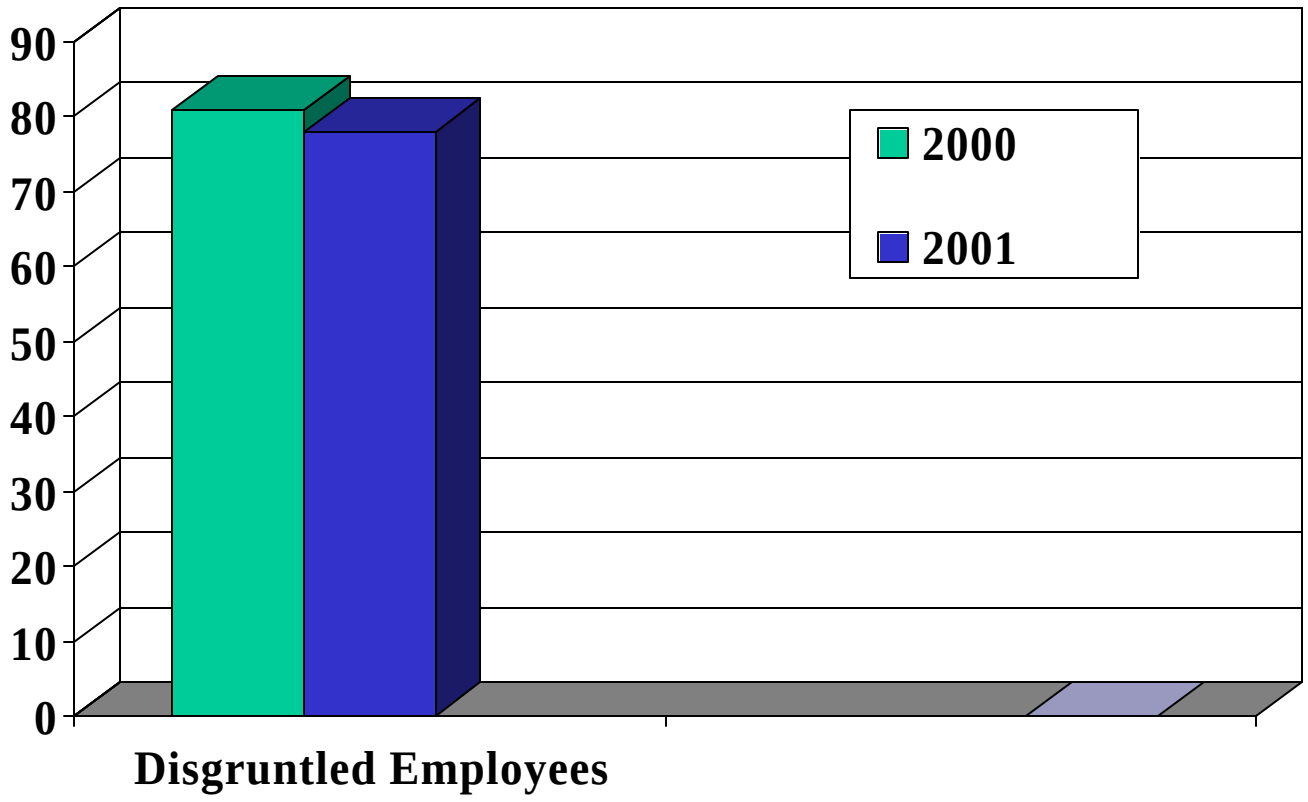
- Web Servers
  - Web Site Security receives relatively little attention yet can provide very easy access for even relatively unskilled hackers.
  - Make sure the material on the web site contains no links back to the main server.
  - Password protect the site.

External Vulnerabilities

- Web Servers
  - Encrypted Password plus token
  - VPN
  - Firewall
  - Remote Ticket

Network Security

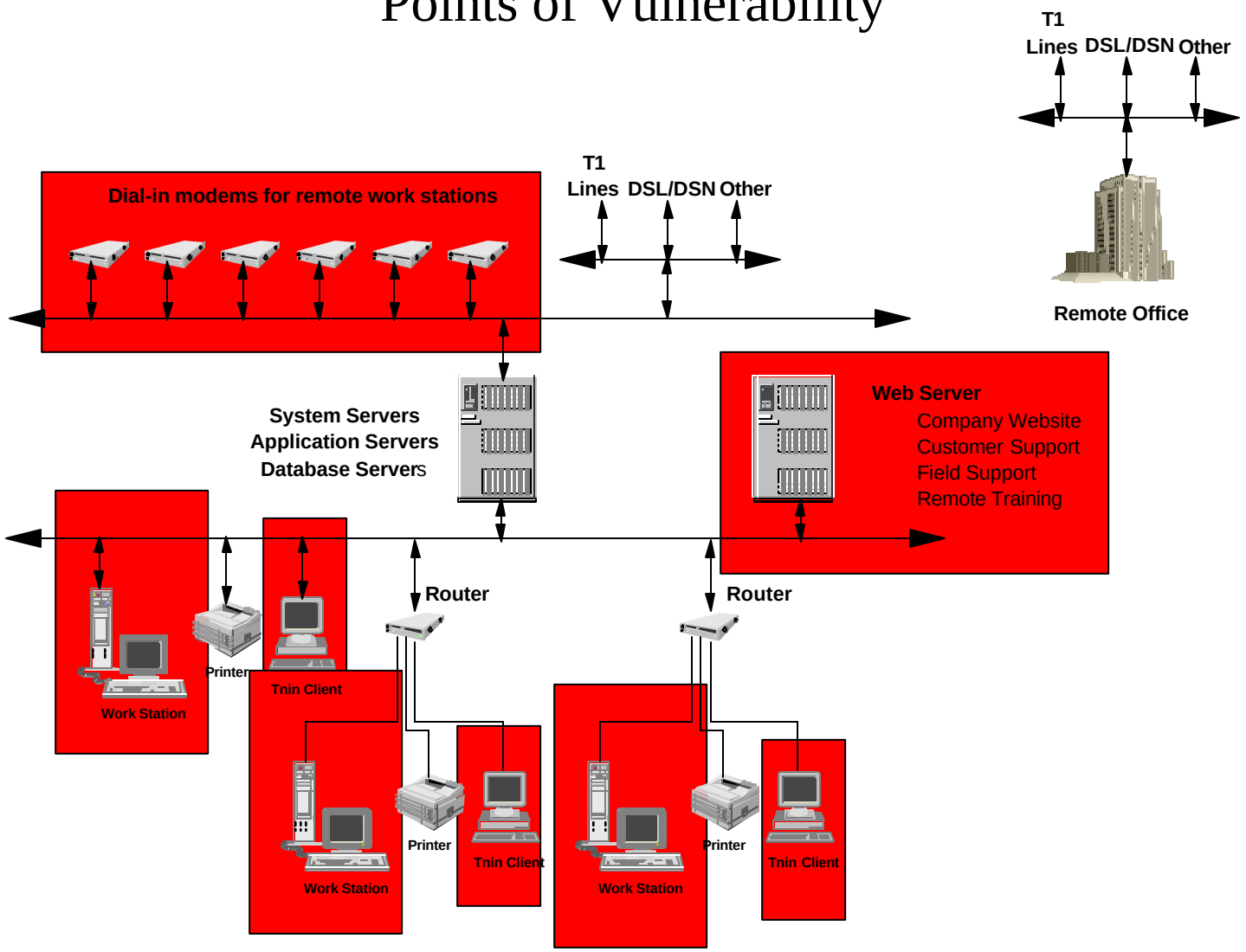
Internal Threats



6th Annual Computer Crime and Security Survey, Computer Security Institute /FBI Survey

Typical Enterprise LAN/WAN

Points of Vulnerability

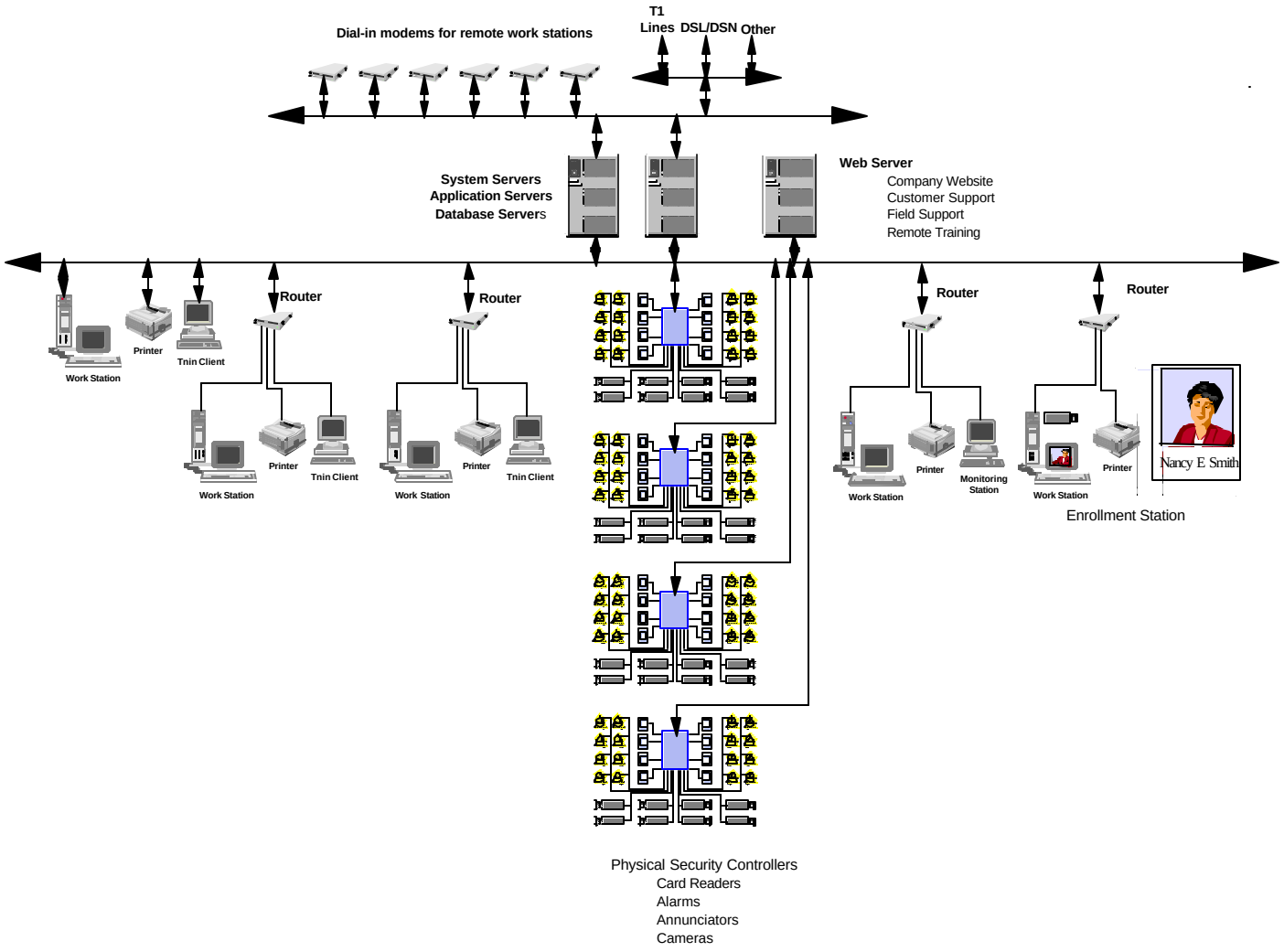


Network and Physical Security Together

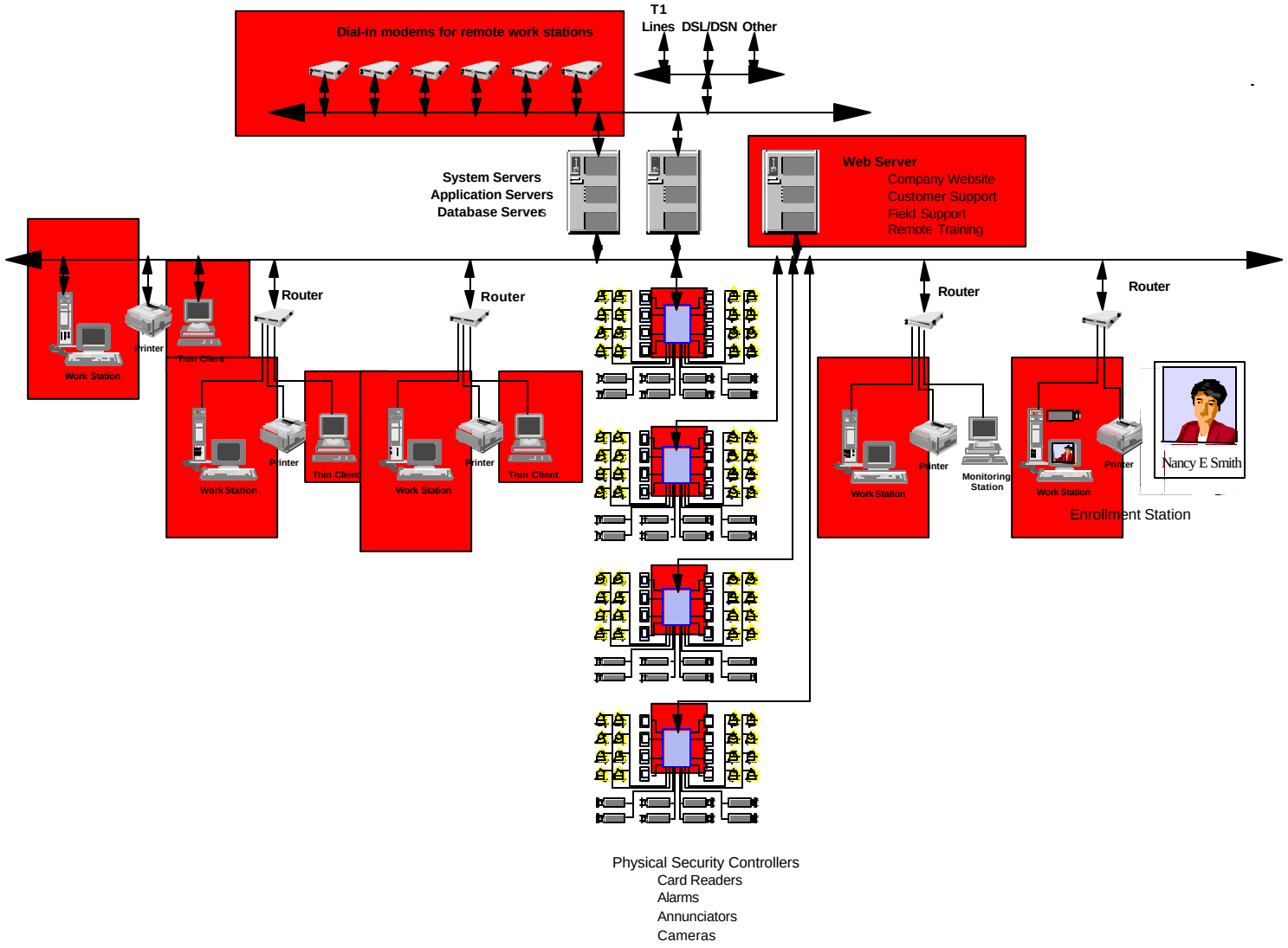
The Integrated System Picture

- The Risks Increase
  - All the risks associated with unauthorized file access plus
  - The additional risk of someone obtaining unauthorized physical access.

Integrated Physical Security and IT Network System



Enterprise LAN/WAN with Integrated Physical Security System



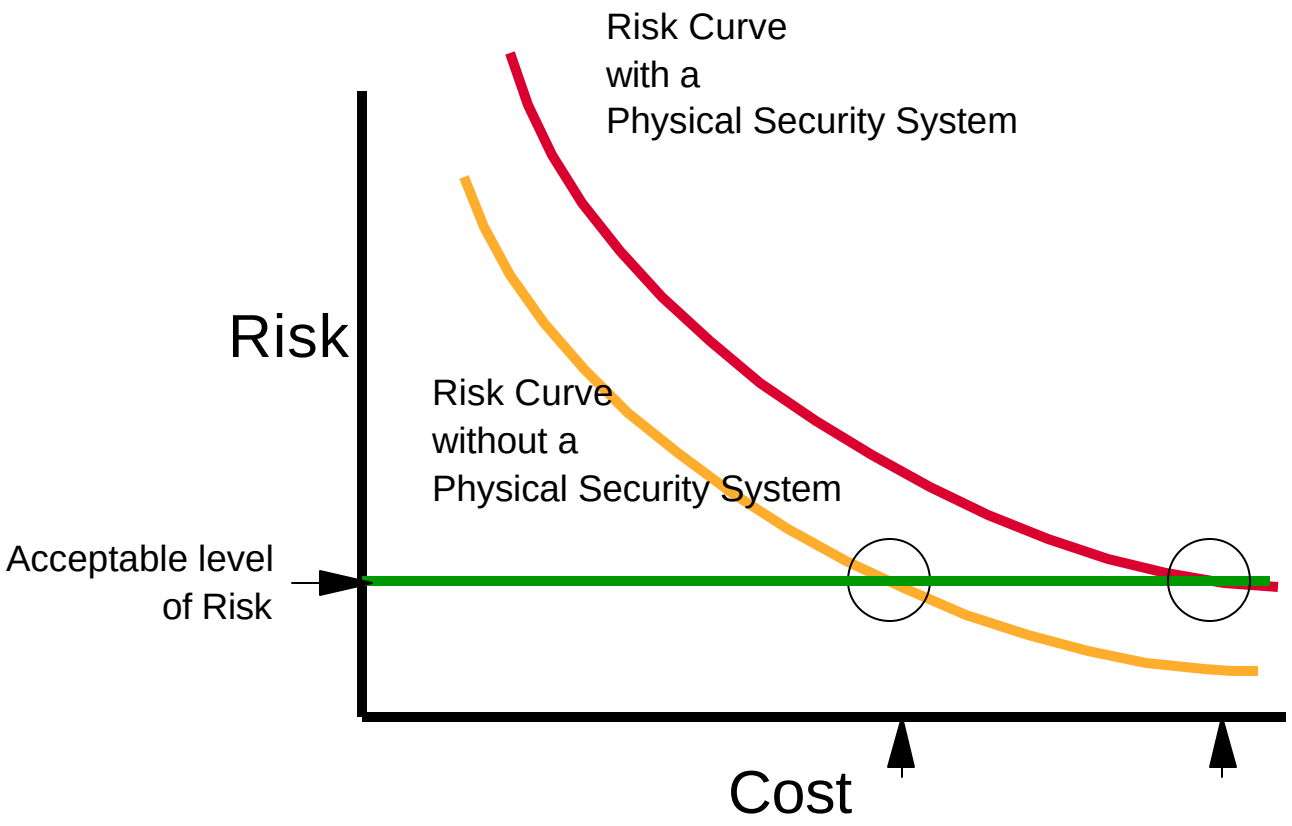
Network Security

Solutions

Network Security

Solutions

Risk vs Cost



Network Security
Solutions

- The three “A”s of successful security
  - Administration
  - Authority
  - Access

Network Security
Administration

- The three most important things for success:
  - Management
  - Management
  - Management

Network Security
Administration

- Physical Security Management and Network Management must work closely together:
  - Each must have a good understanding of and respect for the others objectives.
  - There must be a hand-in-glove working relationship. Good communication is everything.
  - There must be a clear policy and procedure for quickly resolving conflicts.

Network Security
Administration

- **OPRA -**The keys to successful management
  - Smart **Objectives**
    - Specific
    - Measurable
    - Achievable
    - Realistic
    - Time bound
  - A **Plan** to implement these objectives
  - The **Resources** to carry out the plan
  - **Accountability**

Network Security

Authority

- Just as there are access levels and time codes for a physical security access control system the same is required for a network security system.
- For most corporations this is a very hap-hazard process.
- If the physical security system is part of the enterprise network, network access control must be systematic, regulated, and monitored.

Network Security

Access Control

- The network administration system must support access levels and time codes with some method of reporting illegal access attempts by whom, when, and where.

Network Security

Tools of the Trade

- Access Control
  - Anti-Virus Software
  - Firewalls
  - VPN
  - External Ticketing
  - Passwords
  - Biometrics

Network Security

Tools of the Trade

- Authentication:
  - Passwords
  - Tokens
  - Biometrics
    - Fingerprint
    - Hand Geometry
    - Iris Scanning
    - Retinal Scanning
    - Facial Recognition
    - Voice Recognition
  - External Ticketing

Network Security

Tools of the Trade

- Administration
  - Access Control Software
  - Incident Reporting
  - Incident Tracking
  - Policies and Procedures
  - ISO 17799

Networks and Physical Security Systems

- In the end “There are no free lunches”
  - Significant cost savings and ease of operation
    - Versus
  - Significant up-front expense and administrative change.
- The key is “Know what you are getting into!”

Networks and Physical Security Systems

Thank you

William H. Sawyer, Ph.D.